IN THE DISTRICT COURT OF THE UNITED STATES
FOR THE DISTRICT OF SOUTH CAROLINA
GREENVILLE DIVISION

UNITED STATES OF AMERICA,	)	CIVIL ACTION NO.:
	)	
Plaintiff,	)	
	)	
vs.	)	
	)	
112,850.465501 USDT,	)	
	)	
Defendant *in Rem*.	)	

UNITED STATES' COMPLAINT FOR FORFEITURE *IN REM*

The Plaintiff, United States of America, brings this complaint and alleges as follows, in accordance with Rule G(2) of the Supplemental Rules for Admiralty and Maritime Claims and Asset Forfeiture Actions.

NATURE OF THE ACTION

1. This is a civil action *in rem* to forfeit to the United States of America funds in the amount of 112,850.465501 Tether Crypto Currency ("USDT") valued at approximately $112,893.98 USD ("United States Dollars"), ("Defendant Funds"), pursuant to 18 U.S.C. § 981(a)(1)(A) and 18 U.S.C. § 981(a)(1)(C). The United States seeks forfeiture based upon a reasonable belief that the Government will be able to meet its burden of proof at trial to show that the Defendant Funds constitutes, or is traceable to:

a. property involved in wire fraud transactions or attempted wire fraud transactions in violation of 18 U.S.C. § 1343;

b. property involved in money laundering transactions or attempted transactions in violation of 18 U.S.C. § 1956(a)(1)(A)(i), and/or § 1956(a)(1)(B)(i) and/or 1957;

c. property involved in an illegal money transmitting business, in violation of 18 U.S.C. § 1960; and/or;

d. proceeds of some other form of specified illegal activity set forth in 18 U.S.C. § 1956(c)(7) and;

e. proceeds of some other form of specified illegal activity set forth in 18 U.S.C. § 1956(h) and;

f. property involved in money transactions in criminally derived property or attempted money transactions, in violation of 18 U.S.C. § 1957.

JURISDICTION AND VENUE

2. This Court has subject matter jurisdiction over an action commenced by the United States pursuant to 28 U.S.C. § 1345, and over an action for forfeiture by virtue of 28 U.S.C. § 1355. This Court has *in rem* jurisdiction over the Defendant Funds pursuant to:

(a) 28 U.S.C. § 1355(b)(1)(A), because acts or omissions giving rise to the forfeiture occurred in the District of South Carolina; and

(b) 28 U.S.C. § 1355(b)(1)(B), because venue properly lies in this district pursuant to 28 U.S.C. § 1395.

THE DEFENDANT *IN REM*

3. The Defendant Funds consist of 112,850.465501 Tether Crypto Currency USDT valued at approximately $112,893.98 USD, obtained by agents with the United States Secret Service ("USSS") during an investigation into a transnational criminal organization running a law enforcement imposter scheme. The funds were seized from a cryptocurrency

custodial wallet under the control of Binance, identified by account number xxxxNxFN ("Suspect Wallet") and under the name of Arti Gupta ("Gupta").

4. The USSS seized the 112,850.465501 USDT valued at approximately $112,893.98 USD, for federal forfeiture. The Defendant Funds are currently restrained and pending deposit to an account under the control of United States Secret Service.

5. In accordance with the provisions of 19 U.S.C. § 1606, the Defendant Funds have a total domestic value of approximately $112,893.98.

KNOWN POTENTIAL CLAIMANTS

6. The known individuals whose interests may be affected by this litigation are:

a. Arti Gupta who may have an interest in the Defendant Funds because he was the named account holder of the account seized by USSS during this investigation.

BASIS FOR FORFEITURE

7. Pursuant to the pleading requirements of Supplemental Rule G(2)(f), Plaintiff alleges that there is a factual basis to support a reasonable belief that the Government will be able to meet its burden of proof at trial to show that the Defendant Funds are subject to forfeiture to the United States, based in part upon the following:

a. The United States Secret Service and Easley City Police Department were contacted to investigate a report from a victim involved with a Law Enforcement Imposter Scam. In summary, it is common across many of the Law Enforcement imposter scams, when it comes to cryptocurrency, that the fraudsters initially contact the victim using digital

communication, often telephone calls. In these cases, the victim is often convinced that their information has been identified as being involved in a fraud scheme. They are then led to believe that they can avoid an arrest warrant if they pay a particular fine or bond. These funds are typically sent via a crypto currency account provided by the fraudsters. The fraudsters then use pass-through wallets to quickly transfer the currency to avoid seizure by law enforcement.

b. Digital currency (also known as virtual currency or cryptocurrency)[1] is generally defined as an electronic-sourced unit of value that can be used as a substitute for fiat currency (i.e., currency created and regulated by a government). Digital currencies exhibit properties similar to other currencies, but do not have a physical form, existing entirely on the internet. Digital currency is not issued by any government or bank (in contrast with fiat or conventional currencies) and is instead generated and controlled through computer software operating on a decentralized peer-to-peer network, often referred to as the blockchain or public ledger. Digital currency is legal in the United States and accepted for legitimate financial transactions. However, digital currency is often used for conducting illegal transactions or for concealing or disguising the true nature, source, location, ownership or control of illegally obtained proceeds. Bitcoin ("BTC") is one of the most commonly used and well-known digital currencies. Ethereum ("ETH") is another popular and commonly used digital currency.

[1] For purposes of this complaint, the terms "digital currency," "cryptocurrency," and "virtual currency" are used interchangeably and address the same concept.

c. A stablecoin is a digital currency whose market value is attached to or "pegged" to another stable asset. Differing from normal digital currencies, the value of stablecoins are pegged to assets such as fiat currencies like the United States Dollar ("USD") or the Euro, or other types of assets like precious metals or other digital currencies. Stablecoins are thus used to mitigate the volatility in the price of digital currency by mimicking the value of a fiat currency, without actually converting digital currency into fiat. While there are various legitimate uses for stablecoins, they are popular with cyber-criminals who seek to hold digital currency proceeds of crime at a stable or near-fixed value without moving those funds into the legitimate financial system into a fiat currency such as USD. Some examples of stablecoins include:

i. Tether (USDT) was developed by Tether Limited Inc. and is designed to maintain its value at $1.00 USD. USDT can utilize the existing ETH blockchain or the newer TRON ("TRX") blockchain.

ii. Binance USD (BUSD), which was developed by Binance Holdings Limited and Paxos Trust Company, LLC, is designed to maintain its value at $1.00 USD. BUSD utilizes the existing ETH blockchain.

d. A digital currency exchange (an "exchange") is a business that allows customers to trade digital currencies for other digital or fiat currencies. An exchange can be a brick-and-mortar business, or strictly an online business. Both brick and mortar and online exchanges accept a wide variety of digital currencies, and exchange them for fiat and traditional payment methods, other digital currencies, or transfers between digital

currency owners. Most exchanges are located outside the boundaries of the United States in order to avoid regulation and legal requirements, but some popular exchanges operate inside the jurisdiction of the United States. Binance is an example of a popular online exchange that is located outside of the United States but cooperates with and accepts legal process from American law enforcement agencies.

e. A wallet is a means of storing digital currency identified by unique electronic addresses that allows an individual to conduct transactions on the public ledger. To access a wallet on the public ledger, an individual must use a public address (or "public key") and a private address (or "private key"). The public address can be analogized to an account number while the private address is similar to a password used to access that account. Even though the public address of those engaging in digital currency transactions are recorded on the public ledger, the true identities of the individuals or entities behind the public address are not recorded. If a real individual or entity is linked to a public address, however, it may be possible to determine what transactions were conducted by that individual or entity. Therefore, digital transactions are often described as "pseudonymous," meaning they are partially anonymous. Most individuals are identified when they use a digital currency exchanger to make a transaction between digital currency and fiat, or through digital currency exchangers that voluntarily or through legal order, cooperate with law enforcement.

f. On October 21, 2024, C.R. a resident of Easley, South Carolina was contacted by who she believed to be Walmart corporate security. The caller told C.R. that

someone was attempting to use her identifiers to make an online purchase at Walmart. The caller then indicated that she would be transferred to her bank and an investigator. C.R. spoke to numerous individuals believing to be helping her with resolving this potential fraud. She was eventually transferred to someone who claimed to be from the Office of the Inspector General. This individual indicated that the victim had several warrants due to the fraud.

g. The victim became very skeptical at this point and began to question the validity of the callers. The fraudsters offered to have the local police department contact her to verify the validity of the calls. She stated that she would like a call from the Easley Police Department to confirm. Moments later, the victim received a call from a phone number that was spoofed to show the Easley Police Department non-emergency number. The caller provided the name of a true employee of the police department. Both the number and identity are easily found online.

h. It was at this point that C.R. was told she would need to send money through a Bitcoin Automated Teller Machine (BATM) to avoid being arrested. The caller directed her to a particular BATM in Easley and walked her through the process. C.R. was provided the QR code that corresponds to the cryptocurrency address xxxxtHxw, and she proceeded to deposit the equivalent of approximately $5,000.00 USD.

i. United States Secret Service S/A Lea reviewed the transaction history for digital currency wallet xxxxtHxw (“Burn Wallet 1”) in a commercial blockchain analysis platform. His summary revealed that on October 22, 2024, at 12:58 a.m. 0.05186844 BTC

was deposited into wallet xxxxtHxw via transaction hash: xxxxaf06 from a Bitcoin Depot BATM. Based on the information from the victim and because it matched the account information provided to the Easley Police Department, S/A Lea concluded this represented the victim C.R.'s deposit. Approximately 10 minutes later, those funds were quickly sent out to wallet xxxxNxFN ("Suspect Wallet") on October 22, 2024, at 8:08 p.m. via transaction hash: xxx2dlec. See Attachment A.

j. S/A Lea then reviewed the transaction history for digital currency wallet xxxxNxFN (Suspect Wallet) in a commercial blockchain analysis platform. This wallet showed to be hosted on the Binance Exchange and had only been active for 9 months, but during that time it received 56 deposits totaling approximately $471,840.61.

k. On November 21, 2024, S/A Lea reviewed the transaction history in the Suspect Wallet provided by the hosting exchange, Binance:

i. Binance identified GUPTA as the account holder of Suspect Wallet. The account became active in February of 2024. Since that time, the account has received 252 deposits totaling approximately $1,369,047.18 and sent 570 transactions totaling approximately $1,269,058.45. In many instances, the BTC received is quickly converted to USDT and sent back out again. This is not the normal activity in a personal crypto investment account.

ii. Immediately after the deposits occur in BTC, the funds are converted to USDT stable coin via the means of Binance Over the County (OTC) trades

selling the funds. Approximately 37 minutes after receiving the victim funds in the form of BTC, the funds were converted to USDT.

iii. The tracing of digital currency stolen from the victim discussed above shows that after the funds were deposited into the first suspect account Burn Wallet 1, the funds were immediately forwarded on to the Suspect Wallet. The Suspect Account data shows that after the funds are converted to USDT, the funds are often forwarded out to other wallets via the TRON network.

l. The Subject Account bears numerous red flags for a money laundering facilitation account, namely:

i. The volume of transactions in the Subject Account is highly suspicious, with more than $1,000,000 in USD equivalent of digital currency moved through the wallet associated with the Subject Account in less than 9 months;

ii. The Subject Account does not appear to hold digital currency for long, instead rapidly receiving and then retransmitting digital currency, and often in the form of stablecoins;

iii. The Subject Account appears to immediately transfer the funds out through a privacy network called TRON.

m. Special Agent Lea's investigation, records provided by Binance, and his training and experience revealed the Subject Account was used primarily to receive

proceeds of fraud scams involving digital currency stolen from victims and to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds obtained from the scam. The Subject Account further concealed and disguised the nature of the proceeds by combining the numerous deposits and forwarding from the account via the TRON Network. Therefore, there is probable cause to believe the Subject Account was used to facilitate the commission of wire fraud, illegal money transmitting, and money laundering and contains proceeds and property involved in the Subject Offenses of USDT (the Subject Funds).

n. On November 22, 2024, Special Agent Lea obtained a federal seizure warrant for the contents of Binance Account 840934002, in the name of Arti Gupta. Following service of this seizure warrant, Binance released the Defendant Funds consisting of 112,850.465501 Tether Crypto Currency USDT to the United States Secret Service.

8. Based on the information and allegations set forth herein, there is a factual basis to support a reasonable belief that the Government will be able to meet its burden of proof at trial to show that the Defendant Funds constitutes, or is traceable to:

a. property involved in wire fraud transactions, attempted wire fraud transactions, or conspiracy of same in violation of 18 U.S.C. §§ 1343, 1349;

b. property involved in money laundering transactions or attempted transactions in violation of 18 U.S.C. § 1956(a)(1)(A)(i), and/or § 1956(a)(1)(B)(i) and/or 1957;

c. property involved in an illegal money transmitting business, in violation of 18 U.S.C. § 1960; and/or;

d. proceeds of some other form of specified illegal activity set forth in 18 U.S.C. § 1956(c)(7);

e. proceeds of some other form of specified illegal activity set forth in 18 U.S.C. § 1956(h) and;

f. property involved in money transactions in criminally derived property, in violation of 18 U.S.C. § 1957.

CONCLUSION

9. By reason of these premises, and pursuant to 18 U.S.C. § 981(f) and 21 U.S.C. § 881(h), whereby the Plaintiff's right, title and interest in and to the Defendant Funds relates back to the commission of the act giving rise to the forfeiture, the Defendant Funds has become and is forfeited to the United States of America, to be disposed of pursuant to Supplemental Rule G(7)(c) for Admiralty or Maritime Claims and Asset Forfeiture Actions, 18 U.S.C. § 981(d), 21 U.S.C. § 881(e), and other applicable laws.

WHEREFORE, Plaintiff prays that due process issue to enforce the forfeiture of the Defendant Funds, *in rem*; that a Warrant for the Arrest of the Defendant Funds be issued; that due Notice be given to all interested persons to appear, make claim, answer and show cause why the forfeiture should not be decreed; that the Defendant Funds be decreed condemned and forfeited to the United States of America for disposition according

to law; and that Plaintiff have such other and further relief as the Court may deem just and proper, together with the costs and disbursements of this action.

Respectfully submitted,

BRYAN P. STIRLING
UNITED STATES ATTORNEY

By: *s/Carrie Fisher Sherard*
Carrie Fisher Sherard #10134
Assistant United States Attorney
55 Beattie Place, Suite 700
Greenville, SC 29601
(864) 282-2100

June 2, 2025